CLAIMS

Please amend the claims as follows, cancel claim 25 without prejudice and enter new claims 59-66 for consideration.

24. (Currently amended) A method for caching secure content in a Secure Reverse Proxy ("SRP") in [[an]]a secure network, comprising:

coupling at least one SRP among at least one web browser and at least one web server wherein the at least one SRP receives from the at least one web browser requests for establishing a first secure session;

establishing the first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the web browser sends an encrypted request for content to the at least one SRP;

decrypting the encrypted request for content from the at least one web browser at the at least one SRP using the first secure session protocol, wherein the at least one SRP determines that the at least one SRP does not possess the requested content;

establishing a second secure session using a second secure session protocol between the at least one SRP and the at least one web server, wherein the second secure session is maintained;

encrypting the request for content from the at least one web browser using the second secure session protocol;

sending the encrypted request for content to the at least one web server using the second secure session;

receiving the content from the at least one web server at the least one SRP using the second secure session;

decrypting the content using the second secure session protocol;

encrypting said content using the first secure session protocol for sending, using the first session, to the at least one web browser in response to the encrypted request for content;

determining if the requested content is a static content;

encrypting the requested content, if the requested content is the static content, using a third secure session protocol[[;]] for storing the encrypted requested content locally in a memory at the at least one SRP, wherein the third secure session protocol is known only to the at least one SRP; [[and]]

~~retrieving~~decrypting the static content from the memory at the at least one SRP upon subsequent requests for the static content; and

sending the static content to the at least one web server.

Claim 25 (Canceled)

26. (Original) The method of claim 24, wherein storing includes using non-volatile media.

27. (Original) The method of claim 24, wherein coupling includes establishing a dedicated secure line between the SRP and the web server.

28. (Original) The method of claim 24, wherein coupling includes collocating the web server and the SRP.

29. (Original) The method of claim 24, wherein content includes an HTTP page.

30. (Original) The method of claim 24, wherein the first secure session includes Transport Layer Security protocol.

31. (Original) The method of claim 24, wherein the second secure session includes Transport Layer Security protocol.

32. (Original) The method of claim 24, wherein the first secure session includes Secure Socket Layer protocol.

33. (Original) The method of claim 24, wherein the second secure session includes Secure Socket Layer protocol.

34. (Original) The method of claim 24, wherein the first secure session includes Internet Protocol Secure ("IPSec") techniques.

35. (Original) The method of claim 24, wherein the second secure session includes Internet Protocol Secure ("IPSec") techniques.

36. (Previously presented) The method of claim 29, further comprising, before storing the HTTP page, encrypting the HTTP page.

Claims 37-50 (Canceled)

51. (Currently amended) A Secure Reverse Proxy ("SRP") appliance for caching secure static content in a secure network, the SRP appliance comprising:

a processing mechanism;

an encryption and decryption mechanism; and

a tamper-resistant mechanism for storing one or more keys, wherein the one or more keys are known only to the SRP and are used for encrypting the static content before storing the static content in a secure local cache for future requests for the content.

52. (Previously presented) The SRP appliance of Claim 51, wherein the tamper-resistant mechanism includes a tamper-resistant non-volatile card.

53. (Previously presented) The SRP appliance of Claim 51, wherein the local cache includes non-volatile memory.

54. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a secure protocol.

55. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a Secure Socket Layer protocol.

56. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using Internet Protocol Secure ("IPSec") techniques.

57. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a Transport Layer Security Protocol.

58. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is coupled among at least one web server and at least one web browser, wherein the SRP appliance intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server.

59. (New) The SRP appliance of Claim 51, wherein the static content is a banner or a navigation button.

60. (New) The method of claim 24, wherein the static content is a banner or a navigation button.

61. (New) A method for caching secure content over a network comprising:

establishing a first secure session between a client and a proxy server using a first secure session protocol;

encrypting a request for content at the client using the first secure session protocol;

sending the encrypted request for content from the client to the proxy server using the first secure session;

receiving the encrypted request for content at the proxy server using the first secure session;

decrypting the encrypted request for content at the proxy server using the first secure session protocol;

determining that the content is not available at the proxy server;

establishing a second secure session between the proxy server and a web server using a second secure session protocol;

encrypting the request for content using the second secure session protocol at the proxy server;

sending the encrypted request for content from the proxy server to the web server using the second secure session;

receiving the encrypted request for content at the web server using the second secure session;

decrypting the encrypted request for content at the web server using the second secure session protocol;

encrypting the content at the web server using the second secure session protocol;

sending the encrypted content from the web server to the proxy server using the second secure session;

receiving the encrypted content at the proxy server using the second secure session;

decrypting the encrypted content at the proxy server using the second secure session protocol;

determining if the content is a static content at the proxy server;

encrypting the content, if the content is the static content, using a third secure session protocol at the proxy server for storing the static content locally in a memory at the proxy server, wherein the third secure session protocol is known only to proxy server;

encrypting the content at the proxy server using the second secure session protocol;

sending the encrypted content from the proxy server to the client using the second secure session;

receiving the encrypted content at the client using the second secure session;

decrypting the encrypted content at the client using the second secure session protocol; and

decrypting the static content at the proxy server using the third secure session protocol when an additional request for the static content is sent from the client to the proxy server.

62. (New) The method of claim 61, wherein a plurality of clients are each securely connected to the proxy server via a plurality of differing secure session protocols and the proxy server is securely connected to the web server via the

second secure session protocol in order to retrieve secure content requested by the plurality of clients that is not contained at the proxy server.

63. (New) The method of claim 61, wherein the static content is a banner or a navigation button.

64. (New) A method for caching secure content over a network comprising:

establishing a first secure session between a client and a proxy server using a first secure session protocol;

sending an encrypted request for content from the client to the proxy server using the first secure session;

receiving the encrypted request for content at the proxy server using the first secure session;

decrypting the encrypted request for content at the proxy server using the first secure session protocol;

determining that a first part of the content is available at the proxy server and a second part is not available at the proxy server;

establishing a second secure session between the proxy server and a web server using a second secure session protocol to retrieve the second part of the content;

encrypting a second request for the second part of the content using the second secure session protocol at the proxy server;

sending the encrypted second request for the second part of the content from the proxy server to the web server using the second secure session;

receiving the encrypted second request for the second part of the content at the web server using the second secure session;

decrypting the encrypted second request for the second part of the content at the web server using the second secure session protocol;

encrypting the second part of the content at the web server using the second secure session protocol;

sending the encrypted second part of the content from the web server to the proxy server using the second secure session;

receiving the encrypted second part of the content at the proxy server using the second secure session;

decrypting the encrypted second part of the content at the proxy server using the second secure session protocol;

determining if the second part of the content is a static content at the proxy server;

encrypting the second part of the content, if the second part of the content is the static content, using a third secure session protocol at the proxy server for storing the static content locally in a memory at the proxy server, wherein the third secure session protocol is known only to proxy server;

decrypting the first part of the content at the proxy server using the third session protocol;

encrypting the first and second parts of the content at the proxy server using the second secure session protocol;

sending the encrypted first and second parts of the content from the proxy server to the client using the second secure session;

receiving the encrypted first and second parts of the content at the client using the second secure session;

decrypting the encrypted second and first parts of the content at the client using the second secure session protocol; and

decrypting the first and second parts of the content at the proxy server using the third secure session protocol when an additional request for the first and the seconds parts of the content is sent from the client to the proxy server.

65. (New) The method of claim 64, wherein a plurality of clients are each securely connected to the proxy server via a plurality of differing secure session protocols and the proxy server is securely connected to the web server via the second secure session protocol in order to retrieve secure content requested by the plurality of clients that is not contained at the proxy server.

66. (New) The method of claim 64, wherein the static content is a banner or a navigation button.